REMARKS

This response amends claims 10, 12, 16 and 18 to correct minor informalities and adds new claim 22. Support for the new claim can be found, e.g., at original claim 20. Upon amendment, this application will have 4 independent claims (claims 1, 13, 20 and 22) and 20 total claims (claims 1-2, 4-5 and 7-22). Enclosed please find a form for excess claims.

In section 3 of the Office Action, the Examiner objects to claims 10, 12, 16 and 18 due to missing periods at the end. These informalities have been corrected. It is believed that this objection has been overcome.

In section 2 of the Office Action, the Examiner rejects claims 1, 2, 4, 5 and 7-21 under 35 USC 102(e) as being anticipated by Aziz et al. (US Patent No. 6,643,701). These rejections are respectfully traversed.

Aziz et al. fails to disclose, teach, or suggest, *inter alia*, the following features recited by claim 1 of the present application:

"first means, operative in the course of said handshake, to pass to said peer security entity a first indication indicating the services required by the local application entity, to receive back from said peer security entity a second indication indicating the attributes required of the local application entity by the remote application entity for carrying out said services, and to pass first attribute justifications in the form of one or more certificates, to said peer security entity"; and

"second means, operative in the course of said handshake, to pass to

said peer security entity a third indication indicating the attributes required of the remote application entity by the local application entity, and to receive second attribute justifications, in the form of one or more certificates, from said peer security entity".

The present application concerns a security protocol that sits above, and is independent of the transport layer of a communications stack. In other words, there is no one-to-one association between a transport connection and an instance of the security protocol. Such a one-to-one association would encrypt all traffic on the connection. Instead, the security protocol in the claimed invention can be applied to one of multiple channels set up over the same transport connection to a remote entity.

In the claimed invention, the attributes that the local and remote entity have to prove to each other by certificates are not predetermined, but are indicated during the protocol handshake. In the prior art, however, only identity attributes are exchanged during the security protocol handshake. In contrast, in the security protocol handshake in the claimed invention:

(i) the local entity indicates to the remote entity what attributes it wants the remote entity to prove it has;

(ii) the local entity indicates what services it requires from the remote entity and

(iii) in response, the remote entity indicates what attributes it requires the local entity to prove it has (see pages 13-15 of the specification for explanation).

Aziz et al. relates to a system to provide secure communication between a client and a server. Aziz et al. sets up a first secure connection between a client and a relay and a second secure connection between the relay and a target server. The secure connections can be established using the SSL handshake as illustrated in Fig. 1 and described at col. 8, line 20 of Aziz et al. With respect to features of the claimed invention, Aziz et al. discloses nothing more than the admitted prior art described at pages 1-2 of the specification, namely the Netscape SSL protocol as described in US Patent No. 5,657,390 (the "SSL patent") and the TLS variant of SSL standardized by the Internet Engineering Task Force in RFC 2246.

There are many differences between Aziz's SSL protocol and the handshake recited by the claimed invention. For example, SSL is not transport layer independent. SSL requires a one-to-one association with a transport connection (see page 1, lines 18-23 of the specification) and so is closely associated with the transport layer. This is evident from the name that IEFT gave their version of SSL (that is, TLS - Transport Layer Security). It is also evident from the SSL patent. See, for example, col. 13 where the SSL library opens and closes socket connections as required. Socket connections are transport-level connections. In contrast, the claimed invention calls for a security protocol handshake between transport-independent security entities.

Furthermore, according to the claimed invention, the local entity indicates in a security-handshake message what services it requires from the remote entity. This results in the remote entity determining what attributes the local entity must possess to receive those services and

asking for proof of these attributes in another security-handshake message. The local entity then provides certificates to prove it possesses the required attributes in a further security-handshake message.

SSL protocol, however, does not have such feature. The only attribute that the remote server may require of the local client is its identity. If the server wants the client to prove this, it sends the REQUEST-CERTIFICATE messag (see col. 2, lines 9-10 of Aziz, or preferably, col. 29, lines 29-35 of the SSL patent). There is no disclosure in Aziz or the SSL patent that the client should first indicate what services it wants from the server and the server then deciding what attributes the client must possess to receive those services. Thus, Aziz does not disclose or suggest the "first means ... second means" as recited by claim 1 of the present application, as quoted above.

Moreover, according to the claimed invention, the local entity indicates in a security-handshake message what attributes it requires the remote entity to possess and the remote entity responds in another security-handshake message with certificates proving it has those attributes.

SSL does not have this feature. In SSL the remote server provides its identity certificate in the SERVER-HELLO message it sends in response to the local entity's initial CLIENT-HELLO message (see col. 2, lines 1-7 of Aziz, or preferably, see the SSL patent where col. 21, lines 40-55 show the contents of the SERVER-HELLO message). However, there is no opportunity in the security handshake for the local entity to indicate what attributes it requires the server to possess.

Also, the prefered embodiment in the present application is effected in three messages, which is much more efficient than SSL, particularly having regard to the extra functionality it incorporates. Thus, the Applicants respectfully submit that handshake in the claimed invention is novel and non-obvious over the SSL protocol taught in Aziz.

MPEP 2131 states that a "claim is anticipated only if **each and every element** as set forth in the claim is found, either expressly or inherently described, in a single prior art reference," quoting *Verdegaal Bros v. Union Oil Co. of California*, 814 F.2d 628, 631 (Fed. Cir. 1987). Since Aziz et al. nowhere discloses or suggests the above-quoted features of claim 1, the Applicants respectfully submit that claim 1 is patentable. Claims 2, 4-5 and 7-12 are also patentable, at least by virtue of their dependency from claim 1.

Similarly, claim 13 recites, in part, "passing from the local security entity to the remote security entity a first indication indicating the services required by the local system, passing from the remote security entity to the local security entity a second indication indicating the attributes required of the local system by the remote system for carrying out said services, and passing from the local security entity to the remote security entity, first attribute justifications in the form of one or more certificates"; and "passing from the local security entity to the remote security entity a third indication indicating the attributes required of the remote system by the local system, and passing from the remote security entity to the local security entity second attribute justifications, in the form of one or more certificates".

Claim 20 recites, in part, "the handshake further involving: the local security entity indicating to the remote security entity the services and attributes required of said remote system by the local system, the remote security entity indicating to the local security entity the attributes that the remote system requires of the local system in respect of said services, and the exchange of attribute justifications, in the form of certificates, between the security entities". As discussed above, these features are not disclosed or suggested in the cited references. Thus, claims 13 and 20 are also patentable. Claims 14-19 and 21 are patentable, at least by virtue of their dependency from claim 13 or claim 20.

The Applicants have attempted to address all of the issues raised by the Examiner in the Office Action as the Applicants understand them. It is believed that the application is now in condition for allowance. If any point requires further explanation, the Examiner is invited to telephone Troy Cai at (323) 934-2300 or e-mail Troy Cai at tcai@ladasparry.com.

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account No. 12-0415. In particular, if this response is not timely filed, then the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136 (a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to deposit account no. 12-0415.

Enclosed please find a copy of Troy Guangyu Cai's Notice of Limited

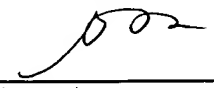
Recognition under 35 CFR 10.9(b) to prepare and prosecute patent applications wherein the patent applicant is a client of Ladas & Parry, and the attorney of record in the applications is a registered practitioner who is a member of Ladas & Parry.

I hereby certify that this correspondence is being deposited with the United States Post Office with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on September 8, 2004

(Date of Deposit)

Troy Guangyu Cai

(Name of Person Signing)

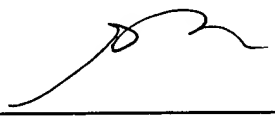


(Signature)

9/8/04

(Date)

Respectfully submitted,



Troy Guangyu Cai
Attorney for Applicant
LADAS & PARRY
5670 Wilshire Blvd., Suite 2100
Los Angeles, California 90036
(323) 934-2300